

Forum:[Hack Forums](#)

Thread: [Load Unmanaged \(Native\) Executable in c#](#)

OFFICIAL MANELE MUSIC - June 12, 2023, 5:08 am

Im wondering how could i load an unmanaged exe/native/c++ executable in .net without dropping it to disk, im hoping someone could help me with a code snippet.

Dread.Reaper - June 12, 2023, 8:31 am

(Jun 12, 2023 05:08 AM)OFFICIAL MANELE MUSIC Wrote: [\[CITE\]](#) Im wondering how could i load an unmanaged exe/native/c++ executable in .net without dropping it to disk, im hoping someone could help me with a code snippet.

Well this explains your interest in my other thread. But why are you trying to use powershell in that thread and C# in this?

Also, protip. Jailbreak GPT to get it to do this for you.

OFFICIAL MANELE MUSIC - June 12, 2023, 12:06 pm

(Jun 12, 2023 08:31 AM)Dread.Reaper Wrote: [\[CITE\]](#) Well this explains your interest in my other thread. But why are you trying to use powershell in that thread and C# in this?

Also, protip. Jailbreak GPT to get it to do this for you.

Gpt always spits out useless, buggy code for me, well i couldnt do it in c# been trying for weeks but i cant do it since c# doesn't really give u access to winapi, tried opening powershell and dumping a script in it to do it, thats why i was interested in your powershell script

Dread.Reaper - June 12, 2023, 3:43 pm

(Jun 12, 2023 12:06 PM)OFFICIAL MANELE MUSIC Wrote: [\[CITE\]](#) Gpt always spits out useless, buggy code for me, well i couldnt do it in c# been trying for weeks but i cant do it since c# doesn't really give u access to winapi, tried opening powershell and dumping a script in it to do it, thats why i was interested in your powershell script

It really boils down to creativity and how you want to deliver.

Is it local, internet based, floppy disk distribution, pidgeon carrier, etc...

Regardless of delivery the most common method is to load or decode the base exes code straight to memory.

So for example an encrypted container on a usb, it would decrypt the exes code straight into the memory, or alternatively like in the powershell example download to a array in the memory.

OFFICIAL MANELE MUSIC - June 13, 2023, 12:08 am

(Jun 12, 2023 03:43 PM)Dread.Reaper Wrote: [\[CITE\]](#) It really boils down to creativity and how you want to deliver.

Is it local, internet based, floppy disk distribution, pidgeon carrier, etc...

Regardless of delivery the most common method is to load or decode the base exes code straight to memory.

So for example an encrypted container on a usb, it would decrypt the exes code straight into the memory, or alternatively like in the powershell example download to a array in the memory.

In .net loading the bytes to a array in memory and then starting it only work with other .net exes, unmanaged exes wont work

Dread.Reaper - June 13, 2023, 12:19 am

(Jun 13, 2023 12:08 AM)OFFICIAL MANELE MUSIC Wrote: [\[CITE\]](#) In .net loading the bytes to a array in memory and then starting it only work with other .net exes, unmanaged exes wont work Perhaps note, I stated Powershell uses a Download array...

NyQuil - June 13, 2023, 12:53 am

should watch some john hammond vids, he has vids in persistent c# malware ran by powershell, i mean with powershell you can literally encrypt a piece of code to run in regs, and it decrypts the c# payload in memory, powershell has all the libs to load a assembly

xloader - June 13, 2023, 11:31 am

(Jun 13, 2023 12:08 AM)OFFICIAL MANELE MUSIC Wrote: [\[CITE\]](#) In .net loading the bytes to a array in memory and then starting it only work with other .net exes, unmanaged exes wont work That isn't entirely accurate; the following serves as a basic proof of concept (POC), you might want to check it out.

unmanaged exe

<https://www.sendspace.com/file/q12cmj>

.Net crypter for it.

<https://hackforums.net/showthread.php?tid=6220104>

OFFICIAL MANELE MUSIC - June 13, 2023, 12:49 pm

(Jun 13, 2023 11:31 AM)xloader Wrote: [\[CITE\]](#) That isn't entirely accurate; the following serves as a basic proof of concept (POC), you might want to check it out.

unmanaged exe

<https://www.sendspace.com/file/q12cmj>

.Net crypter for it.

<https://hackforums.net/showthread.php?tid=6220104>

i still get the same error even with your code, Fatal error. System.AccessViolationException: Attempted to read or write protected memory. This is often an indication that other memory is corrupt.

Im using .net 7, i am running with admin rights, and the xtest.exe file does exist

Code Imports System.IO

Imports System.Runtime.InteropServices

Public Class Test

<UnmanagedFunctionPointer(CallingConvention.Cdecl)>

Public Delegate Function ExecutePE() As Integer

Public Declare Function VirtualAlloc Lib "kernel32" (ByVal lpAddress As IntPtr, ByVal dwSize As UIntPtr,

ByVal flAllocationType As UIntPtr, ByVal flProtect As UIntPtr)

As IntPtr

Public Shared Sub Main()

Dim fileData As Byte() = File.ReadAllBytes("C:\Users\admin\OneDrive\Desktop\xtest.exe")

Dim payload As IntPtr = VirtualAlloc(0, fileData.Length, 12288, 64)

```
Marshal.Copy(fileData, 0, payload, fileData.Length)
```

```
    DirectCast(Marshal.GetDelegateForFunctionPointer(payload, GetType(ExecutePE)),  
ExecutePE)()
```

```
End Sub
```

```
End Class
```

(Jun 13, 2023 11:31 AM)xloader Wrote: [\[CITE\]](#) That isn't entirely accurate; the following serves as a basic proof of concept (POC), you might want to check it out.

unmanaged exe

<https://www.sendspace.com/file/q12cmj>

.Net crypter for it.

<https://hackforums.net/showthread.php?tid=6220104>

XLoader is truly a legend, as he went above and beyond by accessing my AnyDesk to help me fix my error.

xloader - June 14, 2023, 1:46 am

(Jun 13, 2023 12:49 PM)OFFICIAL MANELE MUSIC Wrote: [\[CITE\]](#) i still get the same error even with your code, Fatal error. System.AccessViolationException: Attempted to read or write protected memory. This is often an indication that other memory is corrupt.

Im using .net 7, i am running with admin rights, and the xtest.exe file does exist

```
Code Imports System.IO
```

```
Imports System.Runtime.InteropServices
```

```
Public Class Test
```

```
    <UnmanagedFunctionPointer(CallingConvention.Cdecl)>
```

```
    Public Delegate Function ExecutePE() As Integer
```

```
    Public Declare Function VirtualAlloc Lib "kernel32" (ByVal lpAddress As IntPtr, ByVal dwSize As  
IntPtr,
```

```
                ByVal flAllocationType As IntPtr, ByVal flProtect As IntPtr)
```

```
As IntPtr
```

```
Public Shared Sub Main()
```

```
    Dim fileData As Byte() = File.ReadAllBytes("C:\Users\admin\OneDrive\Desktop\xtest.exe")
```

```
    Dim payload As IntPtr = VirtualAlloc(0, fileData.Length, 12288, 64)
```

```
    Marshal.Copy(fileData, 0, payload, fileData.Length)
```

```
    DirectCast(Marshal.GetDelegateForFunctionPointer(payload, GetType(ExecutePE)),  
ExecutePE)()
```

```
End Sub
```

```
End Class
```

XLoader is truly a legend, as he went above and beyond by accessing my AnyDesk to help me fix my error.

As you can see that the code is working correctly, to identify the issue with your build, kindly compare the settings of my sample with yours.

Dread.Reaper - *June 14, 2023, 3:08 am*

(Jun 14, 2023 01:46 AM)xloader Wrote: [\[CITE\]](#) As you can see that the code is working correctly, to identify the issue with your build, kindly compare the settings of my sample with yours.

Nice to see people still help out around here.